Available from:

SteelCloud, Inc.
www.steelcloud.com
GSA Contract - GS-35F-4085D
703.674.5500

Model 3000MP Bluetooth Smart Card Reader User Guide

for Apple iPhone 3Gs, iPhone 4, iPad and iPad 2

Version 1.3 30000MP
Date: October 13, 2011

Support

For support relating to baiMobile™ Bluetooth Smart Card Readers:

Biometric Associates, Inc
Main Office (410) 252-7210
support@baimobile.com

Field support:
Michael Smith (407) 823-8130 (cell)
msmith@baimobile.com

Contents

Before you get started

This User's Guide is designed for the Apple iPhone™ 3Gs and 4 smartphones and the Apple iPad™ and iPad 2™ tablet with iOS version 4.0 and higher. If you are using another device, the information herein may be different or may not apply. If you have questions, contact your network administrator or email support@baimobile.com.

Proper Care of your baiMobile™ 3000MP Bluetooth Smart Card Reader

Your ***baiMobile*™3000MP Bluetooth Smart Card Reader** is an electronic product similar to a cell phone or MP3 player that may be damaged by excessive moisture, sand, dirt and impact. Taking proper care of your reader is essential for continued, trouble-free operation.

Welcome

The ***baiMobile*™** solution for the Apple iPhone™ and iPad™ includes:

1. ***baiMobile*™ 3000MP Reader**
2. ***baiMobile*™ Bluetooth adapter** (connects to the 30-pin adapter at the bottom of the iPhone/iPad)
3. ***baiMobile*™** libraries (middleware) – files that are provided to application developers and are installed on your iPhone/iPad when the app is installed

This baiMobile 3000MP solution permits you to perform many of the same functions on a mobile device that are available on a desktop PC including:

- digitally sign and decrypt emails and documents
- log on to web sites and network servers that require CAC or PIV authentication
- other applications that require CAC or PIV authentication.

Hardware and Software Requirements

This section describes the minimum hardware and software requirements necessary to use your Reader with an iPhone or iPad.

Hardware Requirements

Note 1:

Your iPhone must be provisioned – that is it must have certain middleware libraries and APIs loaded in order for the baiMobile reader to function. These middleware libraries and APIs are integrated into an app by the software developer and are installed when the app is downloaded and installed. The files do not exist separately. Contact your administrator for provisioning instructions.

Note 2:

Although the iPhone and iPad have a built-in Bluetooth radio, it is not deemed secure by the US Department of Defense. The baiMobile BTA001 Bluetooth adapter must be used for all applications that require access to the ***baiMobile* 3000MP Reader.** The reader will not pair with the iPhone unless 1) the baiMobile Bluetooth adapter is attached to the iPhone and 2) an app is installed that incorporates our middleware libraries and APIs.

Software Requirements

The following software components are required on your iPhone or iPad:

1. iOS version 4.0 or higher
2. an app containing the ***baiMobile*** middleware libraries (check http://www.biometricassociates.com/iphone-reader-supported-operating-systems.html for a complete list of supported applications)

baiMobile™ Middleware Libraries

The ***baiMobile*** middleware libraries consist of files stored on your iPhone™ that allow iPhone applications and network servers to access the digital certificates and other information stored on the Smart Card. The ***baiMobile*** middleware libraries are integrated into various applications such as secure messaging, data at rest encryption and mobile VPN.

Supported Smart Cards

The ***baiMobile*** middleware libraries are designed to support the Common Access Card (CAC) and the Personal Identity Verification (PIV) cards. Other additional middleware libraries may be required to support other smart card types.

baiMobile™ Bluetooth Smart Card Reader Specifications

Specifications	***Description***
baiMobile 3000MP Bluetooth Smart Card Reader	
Hardware Specifications	
Dimensions	62 mm (2.44 in) wide x 110 mm (4.33 in) high x 20 mm (4.79 in) thick
Weight	70g (2.46 oz)
Status Indicator	LCD panel provides connection indication, signal strength, battery capacity, device name, version info, aided pairing. Configurable LED indicators (use/don't use) for connection indication, user attention and LCD backlighting
Battery	Removable PolyFlex cell; rated capacity 580 mAh, normal voltage 3.7v; in low power mode - 3.5mA, (~7 days battery life)
Power On / Off	Power on activated by card insertion and/or front OK button. Power off activated by card removal or application/device security policy.
Charging Port	Mini-B USB (Charger included with Reader)
Wireless Communications	
Communications Protocol	2.4 GHz frequency ISM band. IEEE 802.15.1 (Bluetooth) with full security enabled
RF Transmission range	10 meters
Supported Bluetooth versions	Devices with Bluetooth ver 2.1 and higher
Data Throughput	750 kb/s to 1 Mb/s
baiMobile Middleware Libraries / Security	
Bluetooth & AES	Mode 4: service level security; FIPS 140-2 approved AES-256 encryption overlay
Authentication Method	S/MIME, SSL and PKI
Mobile Device Security	Custom Reader firmware; FIPS 140-2 certified version of the OpenSSL library on reader and device/BTA100 (NIST certification number 1051); Optional integration with mobile security software vendors providing secure messaging, data at rest encryption and mobile VPN
Mobile Operating Systems	
Supported Operating Systems	iPhone OS version 4.0 and higher, Android version 2.2 and higher. (Always confirm device compatibility before purchasing).

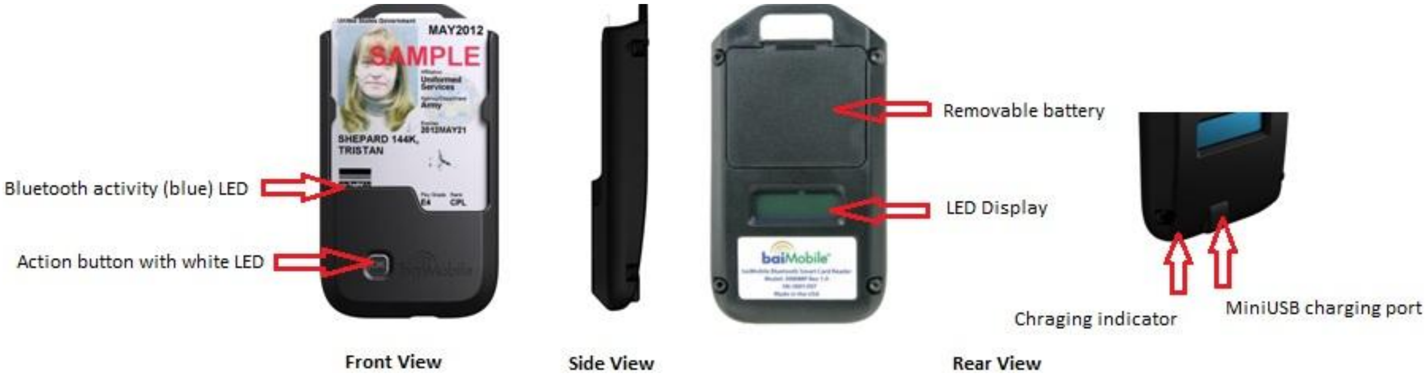
Accessories

Included with your Reader is a charging cable, comprised of a plug and a mini-USB cable.

Reader Basics

Reader Features

Please familiarize yourself with the features of the ***baiMobile* 3000MP Reader.**



- **Blue LED indicator** The blue LED indicator is located on the front portion of the reader, facing the Smart Card. It will flash when the reader's Bluetooth radio is on and is transmitting or receiving data.
- **OK Button with White LED indicator** The OK button is located on the front portion of the reader. Certain functions, such as pairing and reconnecting to the iPhone, require an acknowledgment by the user. A white LED indicator will flash whenever an action or acknowledgment must be performed by the user.
- **Removable Battery/Battery Cover** The reader battery is the only component that will need to be replaced periodically, depending on usage. The battery is rated for 600 charge-discharge cycles, or about two years of normal use. Should the battery need replacing, remove the battery cover and replace the old battery with a new (baiMobile approved) battery. Note: This reader uses a battery custom built for the reader. Inserting a battery other than a baiMobile approved battery will cause serious damage to the reader and will void its warranty.

- ***LED Display*** The LED display is located on the rear of the reader and will display various messages and reader status icons when the reader is powered on.
- ***MiniUSB Charging Port*** The reader's battery is charged using a charging cable and power supply. The power cable is inserted into the miniUSB port located at the bottom of the reader. *Note that the miniUSB port is for charging only and will not support the transfer of data.*

Power consumption

The baiMobile 3000MP smart card reader includes a low-power mode. The operation of the low power modes is complex and based on idle timeouts.

- Reader firmware version 2.2.0 and higher
    - Full power consumption (50-60mA)
        - During pairing
        - During each reader or card command execution duration
            - Each lasts a few seconds, max
    - Idle Power Mode (25mA)
        - Lasts 8 seconds after the last command execution is completed
    - Low Power Mode – connected (3.5mA)
        - Starts 8 seconds after the last command execution is completed
    - Low Power Mode – not connected (3.5mA)
        - Starts immediately after booting is complete (and LCD back light is off)
        - Starts immediately following a disconnection from Bluetooth.
    - For any duration that the LCD back light is on, add another 30mA, but the back light only stays on for short durations (6 seconds, or during pairing, or while holding down the button to see version number, etc.)

To calculate the length of time the reader could continue in any one of these modes, use this equation:

Time in hours = 600 / (mA consumption)

For instance, while connected but in Low Power Mode (3.5mA)

600 / 3.5 = 171 hours (or over 7 days)

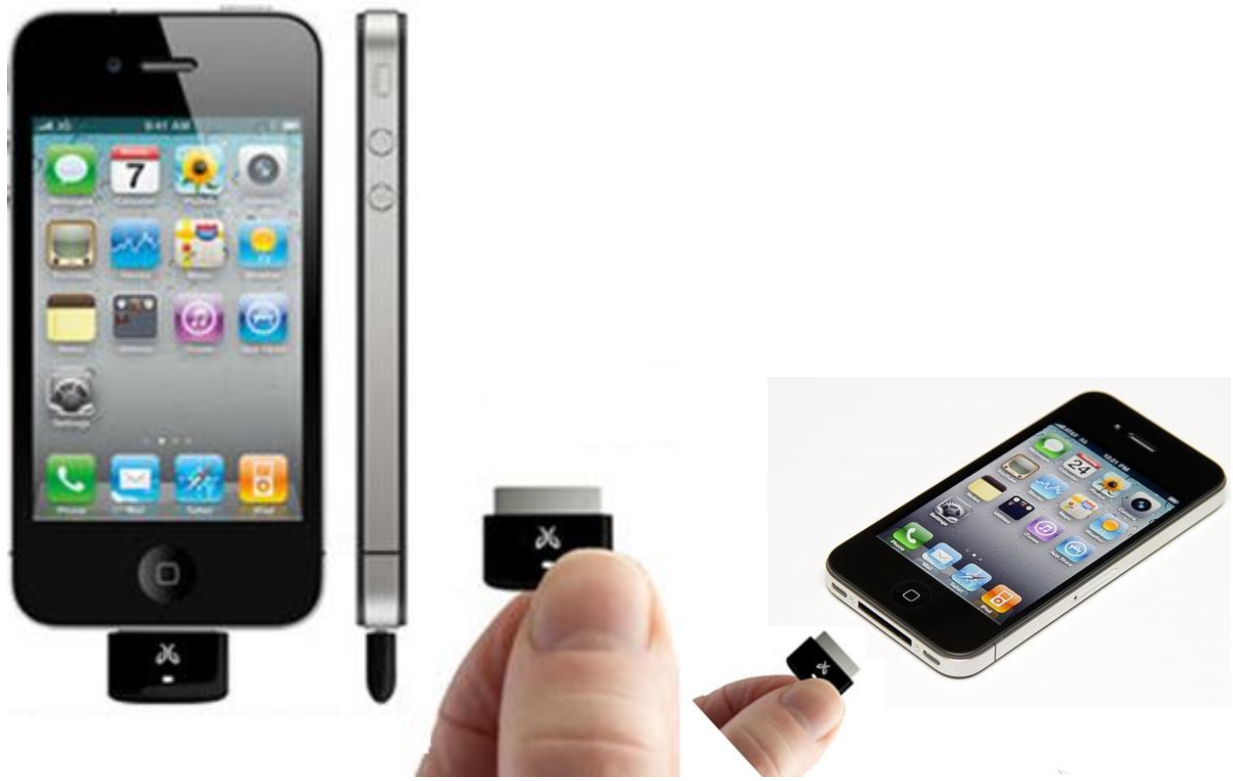
baiMobile Bluetooth adapter

Although the iPhone and iPad have a built-in Bluetooth radio, NSA security recommendations require that all unused Bluetooth profiles be disabled. Since this level of system control is not available in the iPhone OS, an external Bluetooth adapter must be used for all applications that require access to the ***baiMobile* 3000MP Reader.** NOTE: The baiMobile 3000MP Reader will not pair with the native (built-in) Bluetooth radio on the iPhone/iPad

The ***baiMobile* Bluetooth adapter** must be attached to the iPhone in order to:

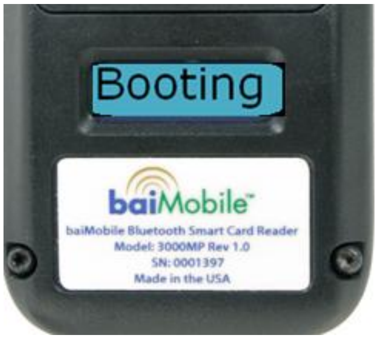
- Pair with the reader;
- Use any iPhone application that requires access to the Smart Card (CAC or PIV) for authentication or to perform cryptographic functions such as signing an email;
- Use any network application or server (including secure web sites) that requires access to the Smart Card (CAC or PIV) for authentication or to perform cryptographic functions such as signing an email;

Insert the ***baiMobile* Bluetooth adapter** with the logo side up into the 30-pin connector at the bottom of the iPhone as illustrated below:

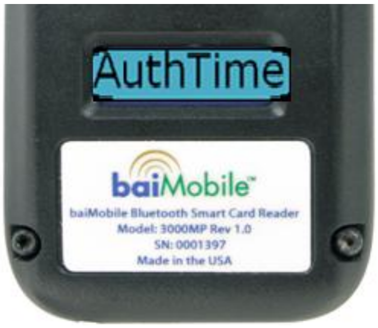


Powering on the Reader

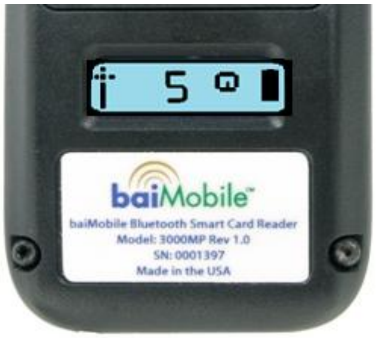
The ***baiMobile* 3000MP Reader** does not have an On/Off switch or button. Your reader is powered on by inserting your CAC into your reader. If your CAC is already inserted in your reader, slide it out and then reinsert the card. You will notice the reader's Home Screen displayed on the LED panel on the back of the reader.



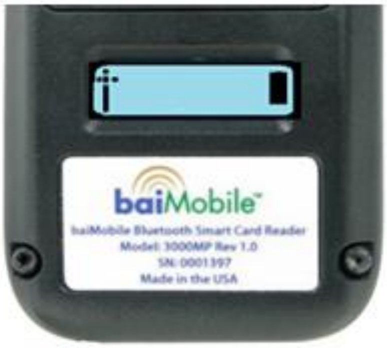
Power On Screen 1 – displayed for about 1.7 seconds when reader is first powered on



Power On Screen 2 – displayed for about 1.7 seconds



Power On Screen 3 – Reader will accept a Bluetooth connection request from an application on your iPhone™ without requiring the user to press the OK button for 5 minutes



Power On Screen 4 –Reader is now powered on and is "listening" for a Bluetooth connection request from an application on your iPhone™. User must first press the OK button to accept a connection request. The reader will stay in this state for approximately 7 days (firmware version 2.02.00 and higher) or until the Smart Card is removed from the Reader, whichever occurs first. If the reader receives a connection request from the iPhone, you may be prompted to authorize the request by pressing and releasing the OK button on the front of the reader.

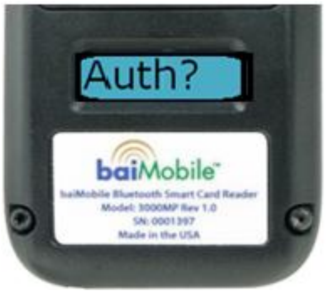
Accepting a Bluetooth connection

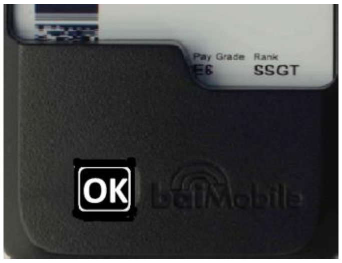
NSA security requirements state that the user must accept (acknowledge) all Bluetooth connection requests from his or her mobile device.

Examples:

- When a client application on the mobile device needs to establish a Bluetooth connection to the reader to access information (certificates) residing on the Smart Card
- When a client application on the mobile device requires that the user acknowledge an action (digital signing) involving the Smart Card

In such cases, the reader will display a message prompt such as "Auth?" and the white LED beneath the OK button will flash repeatedly until the OK button is pressed.





Powering off the Reader

Your reader will automatically power off if any of the following occur:

- Your smart card is removed from your reader
- The reader's battery runs out
- The reader times out (a configurable setting)

When the reader is powered off, nothing will be displayed in the LED panel.

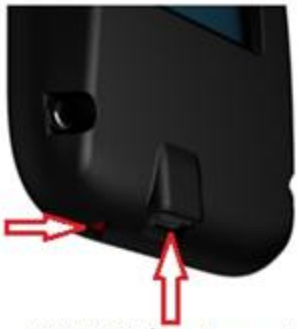
Charging the Reader

Your charging cable separates into a plug end and a mini-USB cable. You may charge your reader using the charging cable plugged into an electrical wall outlet or use just the mini-USB portion of the charging cable to connect between your reader and a USB port on a computer.

It is recommended that the reader be charged whenever the battery status icon on the reader indicates that the reader battery level is less than 20%. The reader should be charged from an AC power source using the supplied charger and cable. A red LED on the bottom of the reader will illuminate indicating that the reader is charging. Once the red LED is no longer illuminated, the battery is fully charged and the charging source should then be removed from the reader.

Wall Charger

USB Charging Cable



MiniUSB charging port

During charging, a red LED on the bottom of your reader will indicate that the battery is being charged. When the red LED turns off, your reader battery is fully charged.

NOTE: Most smartphone charging cables with a mini-USB-a connector will also charge your reader.

Upgrading the Reader Firmware

The baiMobile 3000MP Bluetooth Smart Card reader contains upgradeable firmware. The feature extends the functionality of your Reader in the following areas:

- *Security Policies:* Changes in security policies may require a firmware update.
- *OS Releases:* New versions of the iPhone/iPad operating system may require a firmware update.
- *Smart Card Types:* Support for new smart card types may require a firmware update.
- *Power Modes:* Improvements in the reader's power consumption may require a firmware update.
- *Device Support:* New devices may require a firmware update.
- *Bluetooth Stack Support:* Support for additional Bluetooth stacks may require a firmware update.
- *Additional OS Support:* Support for additional operating systems (such as Windows 7) may require a firmware update.
- *Application Support:* Certain applications may require a firmware update.

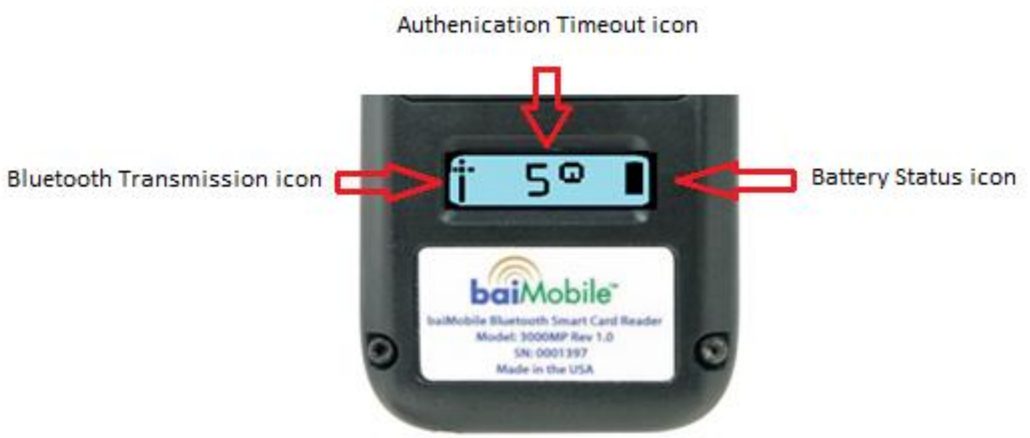
BAL will have a firmware upgrade app available in the iTunes App Store in November, 2011.

LED Panel Icons

Home Screen

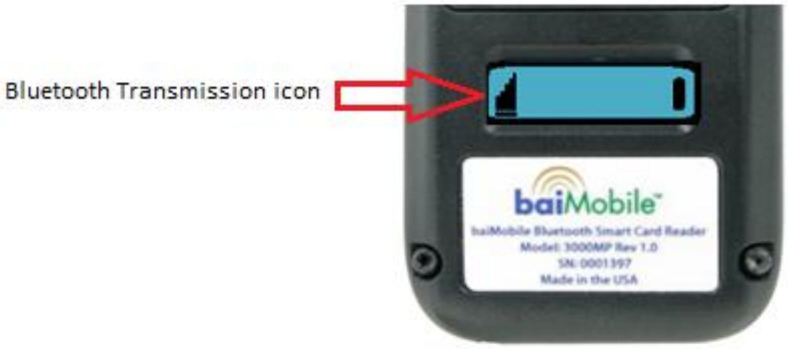
The Home Screen is displayed on the reader's LED panel when the reader is first powered on. The display indicates the following:

- Reader's Bluetooth transmission status: (On / Transmitting)
- Reader's Authentication Timeout status
- Reader's battery power status: (see *Battery Status Icons*)


Authenication Timeout icon
Bluetooth Transmission icon
Battery Status icon
5
baiMobile
baiMobile Bluetooth Smart Card Reader
Model: 3000MP Rev 1.0
SN: 0001397
Made in the USA

Data Transfer Screen

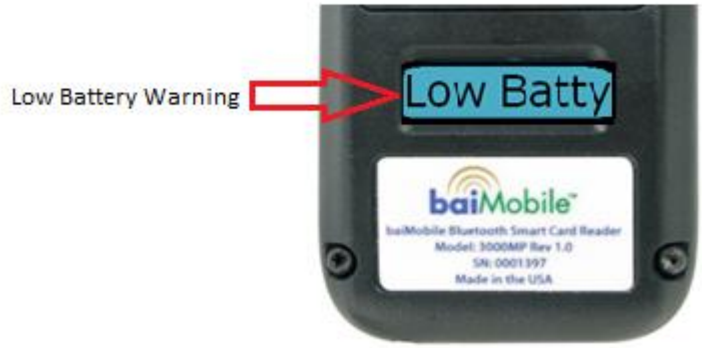
The Data Transfer Screen is displayed on the reader's LED panel when there is data being transferred between the iPhone and the reader over a secure Bluetooth connection.


Bluetooth Transmission icon
baiMobile
baiMobile Bluetooth Smart Card Reader
Model: 3000MP Rev 1.0
SN: 0001397
Made in the USA

Battery Status Icons

The reader's Battery Status Icon will display the remaining charge remaining in the reader's battery, as shown below:

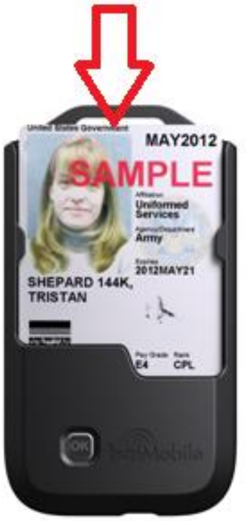
When the battery reaches 5% charge, the Low Battery warning will be displayed. You should charge your reader when the battery reaches about 20% - 40%, depending on your anticipated activities what will require connectivity to your reader, such as accessing email or another application that requires smart card authentication.



Inserting a CAC or PIV card

As noted above, the reader does not have a power on or off button. Insert your CAC or PIV smart card into your reader, with the front of the card facing you, will power on the reader. Removing the CAC or PIV card will power off the reader.

NOTE*:* When used in the Bluetooth mode, the reader's radio functions are only enabled when your CAC or PIV is firmly inserted into the reader as shown below.



Insert your smartcard as shown

Battery

Your reader contains a removable, rechargeable battery. This battery is a custom battery, built specifically for the baiMobile 3000MPReader. In the event that your reader’s battery no longer holds a charge, please contact support@baimobile.com for a replacement battery.

Pairing

Pairing Basics

Before you can use your baiMobile 3000MP Reader, it must be securely paired with your iPhone or iPad. The Bluetooth pairing process involves exchanging a randomly generated number used by both your iPhone™ and your reader for secure Bluetooth communications. This and other security measures insure that Bluetooth communications between your reader and your phone cannot be intercepted by a third party.

The ***baiMobile 3000MP Reader*** utilizes the Secure Simple Pairing Numerical Comparison model, which is standard in most devices that have Bluetooth version 2.1 and higher. During pairing, a six digit number will be displayed on your iPhone screen and on the reader's LED display. You must compare both numbers and confirm that they match.

Before You Begin

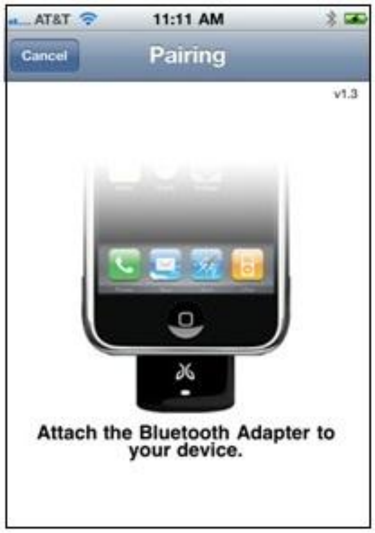
A few things to remember before pairing:

- The pairing is between the reader and the ***baiMobile* Bluetooth adapter** – not between the reader and the iPhone or iPad.
- The reader may only be paired with one Bluetooth adapter at any one time.
- The Bluetooth adapter may only be paired with one reader at any one time.
- Neither the reader nor the Bluetooth adapter will support multiple or simultaneous pairings.
- Be sure that you have fully charged the iPhone and reader before starting pairing
- Have both your CAC/PIV card and Bluetooth adapter handy.

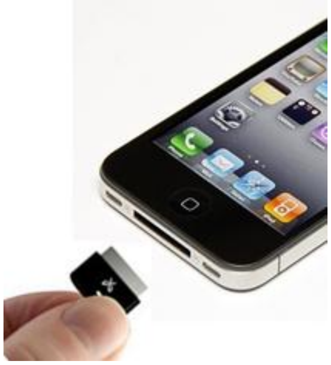
NOTE: You must have an application installed first on your iPhone or iPad that supports the baiMobile 3000MP Reader (such as Good Mobile Messaging). The reader will not pair with an iPhone or iPad otherwise. Please check our web site for a list of supported applications http://www.biometricassociates.com/iphone-reader-supported-operating-systems.html

Your iPhone ***Your Reader***

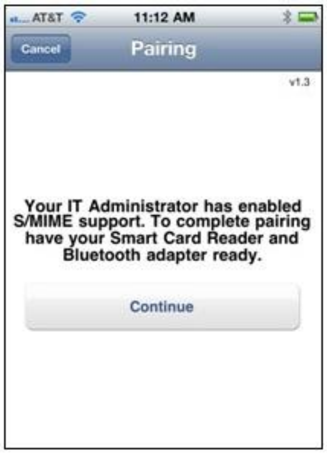
1. You will be prompted to insert the baiMobile Bluetooth adapter as shown (below)



Attach the Bluetooth Adapter to your device.



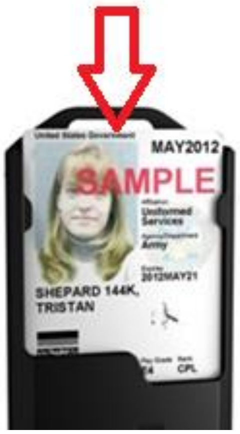
2. As soon as the Bluetooth adapter has been inserted, the next screen will appear on your iPhone.
<u>Do not</u> press *Continue* at this point.



Your IT Administrator has enabled S/MIME support. To complete pairing have your Smart Card Reader and Bluetooth adapter ready.

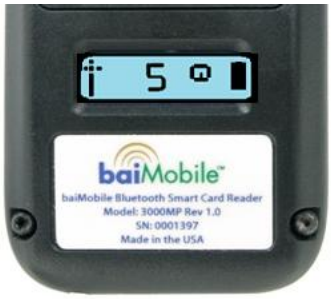
Your iPhone ***Your Reader***

3 Insert your Smart Card into the reader as shown.



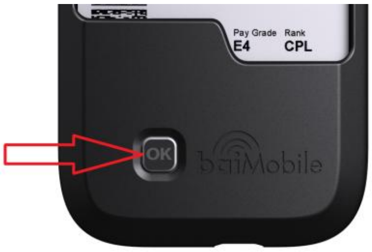
4. The reader's LED panel displays ***Booting*** for about 1.7 seconds, then displays ***AuthTime*** for about 1.7 seconds.

5. Next, reader's LED panel displays the reader Home Screen.



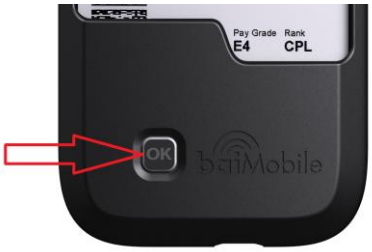
Your iPhone ***Your Reader***

6. On your reader, press and hold the OK Button as shown (below). The LED display now shows the reader firmware version for about five (5) seconds, then displays ***Lift Btn.*** Now release the OK Button.



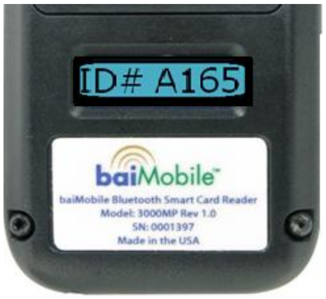
7. The reader’s LED panel will now display ***New Pair?*** for about six (6) seconds.

8. Now press and release the OK Button while the ***NewPair?*** prompt is displayed on the LED panel.

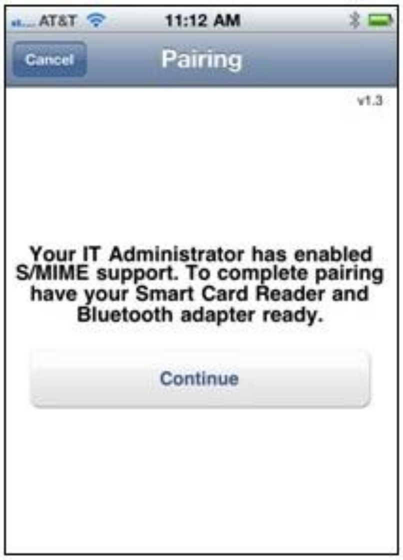


Your iPhone ***Your Reader***

9. The reader is now discoverable by the iPhone and will remain in this state for about ninety (90) seconds. The LED panel now displays the last four numbers of the reader’s unique Bluetooth address.



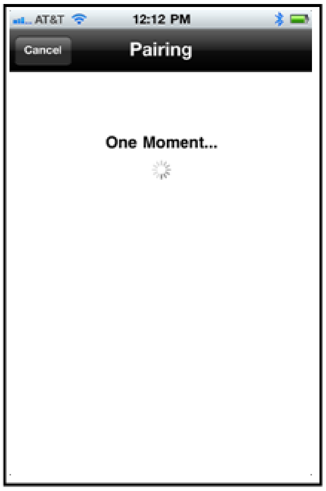
10. On your iPhone, press ***Continue***.



Your IT Administrator has enabled S/MIME support. To complete pairing have your Smart Card Reader and Bluetooth adapter ready.

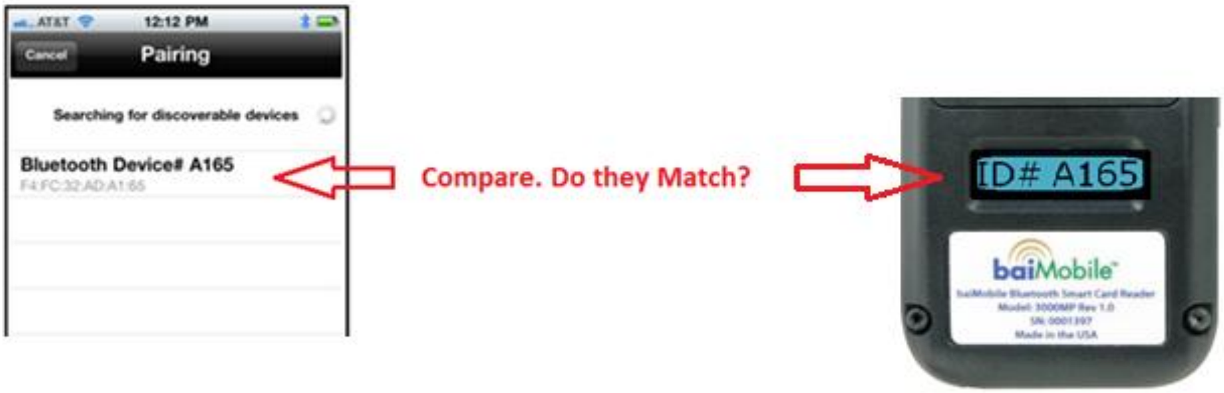
Your iPhone ***Your Reader***

11. Your iPhone will now attempt to discover the reader. Both your reader and iPhone should be in close proximity to each other. Pairing should be done in a secure environment and not in a public area.



One Moment...

12. Your iPhone will now display a list of compatible Bluetooth devices that it has discovered*.* Compare the Bluetooth device ID# displayed on your iPhone with the device ID# displayed on your reader. If the ID numbers match, select the Bluetooth Device highlighted.



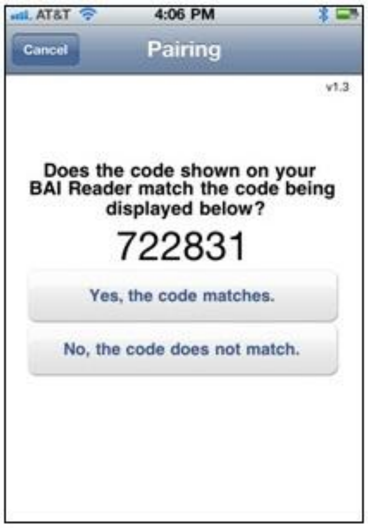
Searching for discoverable devices

Bluetooth Device# A165
F4:FC:32:AD:A1:65

Compare. Do they Match?

Your iPhone **Your Reader**

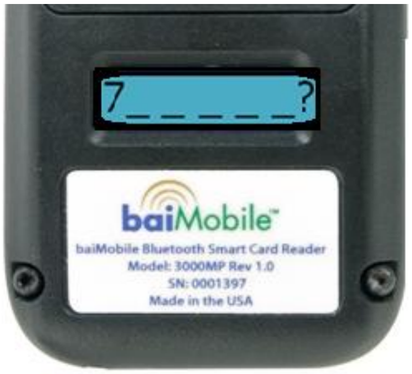
13. Next, the iPhone will display the randomly generated pairing code. Look at the code now displayed on the reader’s LED display.



Does the code shown on your BAI Reader match the code being displayed below?

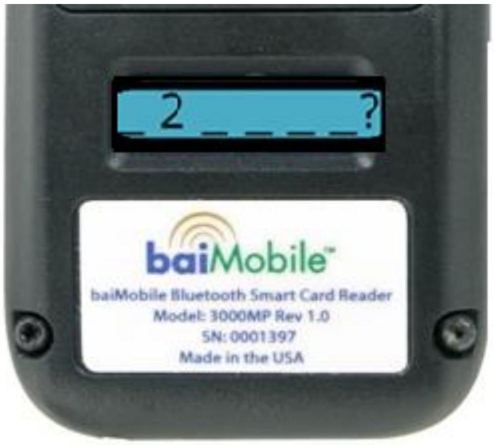
722831

14. Compare the first number of the pairing code displayed on the phone. Compare that number (in this example “7”) with the number displayed on the reader’s LED panel. If they match, press the OK button.



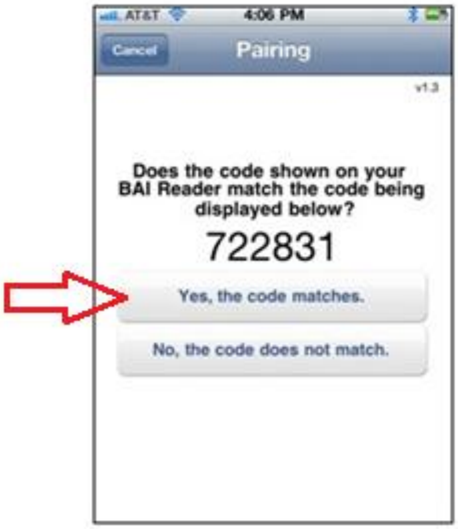
Your iPhone ***Your Reader***

15. Compare the second number of the pairing code displayed on the phone. Compare that number (in this example "2") with the number displayed on the reader's LED panel. If they match, press the OK button.



16. Repeat these steps until you have accepted all six numbers on the Reader.

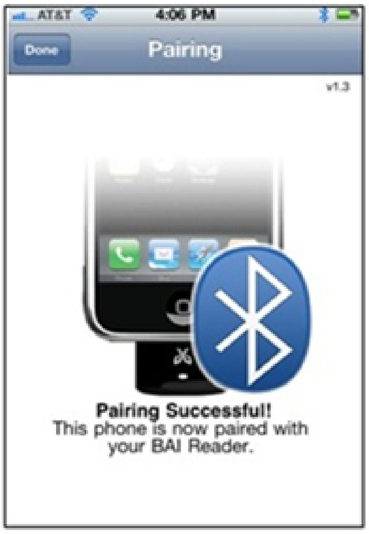
17. Now, press ***Yes, the code matches*** on the iPhone.



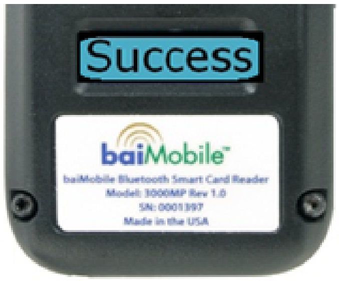
Does the code shown on your BAI Reader match the code being displayed below?

722831

18. You will now see the confirmation messages below on your iPhone and your reader.



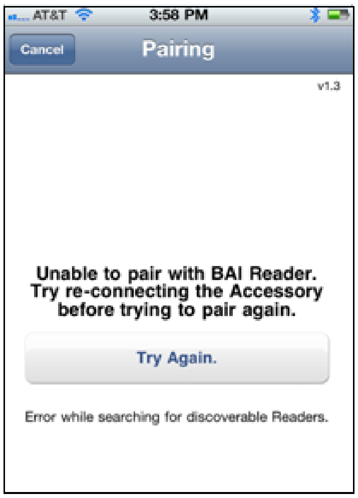
Pairing Successful!
This phone is now paired with your BAI Reader.



Troubleshooting

First, make sure that both your iPhone and reader are fully charged. Both the iPhone and the reader have defined periods of discoverability. These "windows" of discoverability are about 10 seconds on the iPhone and about 90 seconds on the Reader. If either of the discovery windows time out before the devices discover each other, pairing will fail and the process must be restarted.

If you receive the following message on your iPhone, "the iPhone did not successfully pair with the reader", you will need to repeat steps 1-18.



Unable to pair with BAI Reader. Try re-connecting the Accessory before trying to pair again.

Error while searching for discoverable Readers.

PAIRING FAQ

Why do I need the Bluetooth adapter when the iPhone and iPad have built-in Bluetooth?

There are two primary reasons:

- The 3000MP Reader uses the Bluetooth serial port profile to connect to other devices. The iPhone and iPad do not support Bluetooth serial port profile connections.
- NSA and DISA require that all extraneous (unused) Bluetooth profiles be disabled as a security precaution. Since this level of granularity is not available in iOS 4.x for the iPhone's native Bluetooth radio, an external Bluetooth adapter is required for communications with the Smart Card reader.

Can I still use my iPhone's internal Bluetooth radio for connections to other devices, such as a headset?

Check with your network administrator or security officer. The US Department of Defense recommends that the native Bluetooth radio be turned off at all times as a security precaution.

Can I pair my reader to an iPhone or iPad if while the reader is charging?

No.

Index

baiMobile™ Bluetooth Smart Card Reader

Second Edition

Every effort has been made to ensure the accuracy of this manual. However, Biometric Associates, LP makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Biometric Associates, LP shall not be liable for any errors or for incidental or consequential damages with the furnishing, performance, or use of this manual or the examples herein. The information in this document is subject to change without notice.

Windows Mobile® and Microsoft Exchange ActiveSync® are registered trademarks of Microsoft®. Other brand and product names mentioned in this manual may be trademarks or registered trademarks of their respective manufacturers. The information contained herein is subject to change without notice. Revisions may be issued to advise of such changes and/or additions.

Trademarks

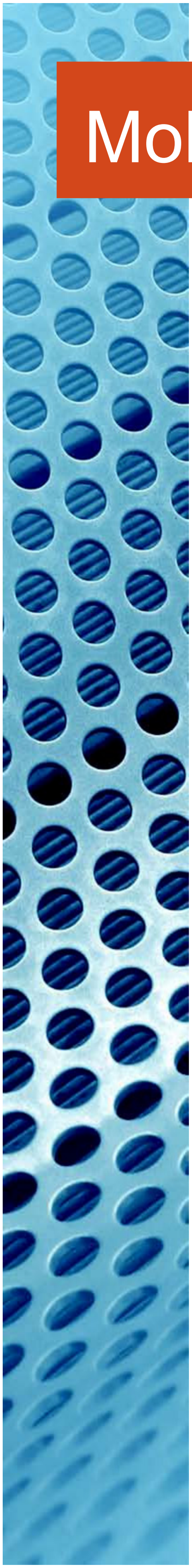
BAL and baiMobile are registered trademarks of Biometric Associates, L.P.

Biometric Associates, LP

Washington Area Office
9475 Deereco Road, Suite 304
Timonium, MD 21093

Maine Office
21 Main Street – Suite 102
Bangor, ME 04401

The BAL Technical Support team understands the importance of prompt responses to customers. That is why Biometric Associates, LP is committed to delivering top quality, high-level support to all of its customers in a timely and effective manner. Current BAL Technical Support is available at: support@baimobile.com .



MobileWorks™ DE for Good

iOS and Android STIG-Compliance!

SteelCloud® and Good Technology™

MobileWorks™ DoD Edition for Good

STIG-Compliant Platform for Deploying iOS and Android Devices

The Next Level of Mobility

DoD adoption of Apple iOS and Google Android mobile devices introduces IT to new device mobility protection and management challenges. SteelCloud and Good Technology are working closely to meet these challenges with MobileWorks for Good and the Good for Government™ product suite.

Fast and DoD-Ready

MobileWorks DoD Edition (DE) for Good is the quickest, least risk, and most cost-effective way to implement Good for Government in a STIG-compliant environment.

Why spend valuable resources and budget deploying iOS and Android mobility management, and engineering your environment to be STIG-compliant? MobileWorks DE for Good deploys STIG-compliant iOS and Android mobility management to production in less than 60 minutes!

MobileWorks DE for Good

MobileWorks DE for Good is available as either a plug & play integrated appliance or a VMware-based virtual solution that comes pre-loaded with Good Technology's Good for Government software, hardened Windows Server OS, and SteelCloud's unique automated set-up and installation facility.

MobileWorks is the newest member of SteelCloud's unique STIG-compliant mobility solutions, engineered to implement the security guidelines mandated by Defense Information Security Agency's (DISA) STIGs to ensure compliance with all applicable environment and application STIGs.

Any size DoD organization can deploy and support a new STIG-compliant Good environment at a fraction of the cost, time, and resource commitment required by manual implementation. To maximize server availability and streamline ongoing maintenance tasks, MobileWorks DE for Good also delivers advanced management features including EverAvail™ Double-Take™ for high availability/failover and disaster recovery/COOP.

The VeriScan™ Advantage

SteelCloud's years of experience in developing and implementing mobile application appliance solutions has shown us that issues with the user environment can be the largest factor in implementing a solution on time and on budget. To address this critical need SteelCloud developed VeriScan. VeriScan is a revolutionary application built to ensure that the user environment is ready for a rapid MobileWorks installation. VeriScan identifies and validates ten critical installation prerequisites necessary to implement Good including firewall port communications, database connectivity, Microsoft Exchange communications, and Active Directory permissions. VeriScan is a critical component in SteelCloud's plug and play methodology and is included with every MobileWorks solution, ensuring a trouble-free installation – the first time!

Benefits

- **Reduces implementation time to less than 60 minutes vs. weeks or months.**
- **Eliminates the risk of non-compliance.**
- **Avoids the learning curve to install & deploy Good for Government is a STIG-compliant environment.**
- **Standard configuration for all deployments.**
- **Eliminates installation & deployment errors.**
- **Simplifies maintenance/support tasks.**

Features

- **Delivered as a COTS solution.**
- **Available as an appliance or VMware-based virtual solution.**
- **Automated one-hour installation.**
- **Flexible installation options to match system configuration.**
- **Powerful EverAvail Double-Take appliance & server high availability and failover.**
- **STIGs are implemented for:**
  - **Wireless, (incl. the security checklist)**
  - **Windows Server OS**
  - **NET Framework**
  - **SQL**
- **Supports Microsoft Server 2008, Microsoft Exchange Server, SQL Server & SQL Express.**

Rely on SteelCloud

Each military service and many DoD agencies have deployed SteelCloud mobility appliances and VMware solutions to speed productivity to users. In each case, administrators were able to start initializing mobility devices within hours of opening our box.

MobileWorks™ DE for Good

High Availability with EverAvail Double-Take

From installation to operation to recovery, MobileWorks is much more than a Good Appliance. MobileWorks' innovative EverAvail™ utilizes the Double-Take® application and server high availability and backup solution to protect the Good for Government implementation and your users from system failure and information loss in the event of a primary system shutdown.

EverAvail Double-Take includes such features as:

- automated physical and virtual machine failover
- protected data compression to improve transfer speed
- centralized reporting and analysis
- email notification

to ensure minimal downtime and complete protection of your mission-critical mobility device management systems and data.

The STIG*360* Customer Support Advantage

The SteelCloud STIG*360* maintenance and support program guarantees that MobileWorks DE for Good customers remain current with the latest DISA STIGs that apply to MobileWorks.

STIG*360* includes pro-active STIG update notifications for Wireless, Windows Server, .NET and SQL and an on-line customer portal for access to MobileWorks DE for Good STIG Implementation Guides. STIG*360* also includes MobileWorks DE for Good Appliance software support, 8x5 telephone support and software image upgrade/replacement services.

With STIG*360*, DoD Information Assurance personnel and Good for Government Administrators have the tools and proactive notification they need to remain compliant with the latest DISA mandated STIGs.

MobileWorks VMware Edition for Good

MobileWorks DE-VM for Good is an enhanced virtual implementation of the MobileWorks DE for Good appliance that supports virtual platform advantages such as server consolidation, test and development, manageability and security in a virtual Good for Government environment. The MobileWorks VMware solution easily installs in an existing VMware infrastructure to create a STIG-compliant Good for Government environment that leverages the server's IT policies.

SteelCloud's virtual appliance also includes EverAvail Double-Take, the unique software suite for appliance and server high availability, failover and disaster recovery.

No matter how Apple iOS and Google Android mobile devices introduce change to your internal IT support resources, you can be confident that MobileWorks DE for Good will deliver the performance, reliability, protection and compliance your agency requires for secure mobile device communications.

MobileWorks DoD Edition for Good

STIG-Compliant iOS and Android Mobility Device Management

Model	Part	Appliances	# of Users	CPU	Memory	Form Factor HxWxD	Included Software
E2400	SCLD-MW-GDDE-E2446A	Single	500 users/GMM	Intel Xeon	4 GB	1U	Good for Government** EverAvail Double-Take** Windows Server OS***
	SCLD-DUAL-GDDE-E2446A	Dual HA Pair	3000 users/GMC	1 Quad Core		1.67" x 17.1" x 15.5"	
E4400	SCLD-MW-GDDE-E4446A	Single	1000 users/GMM* 6000 users/GMC*	Intel Xeon	4 GB	1U	
	SCLD-DUAL-GDDE-E4446A	Dual HA Pair		1 Quad Core		1.69" x 17.09" x 24.69"	
	SCLD-MW-GDDE-E4486A	Single		Intel Xeon	8 GB	1U	
	SCLD-DUAL-GDDE-E4486A	Dual HA Pair		1 Quad Core		1.69" x 17.09" x 24.69"	
E4800	SCLD-MW-GDDE-E4886A	Single		Intel Xeon	8 GB	1U	
	SCLD-DUAL-GDDE-E4886A	Dual HA Pair		2 Quad Core		1.69" x 17.09" x 24.69"	

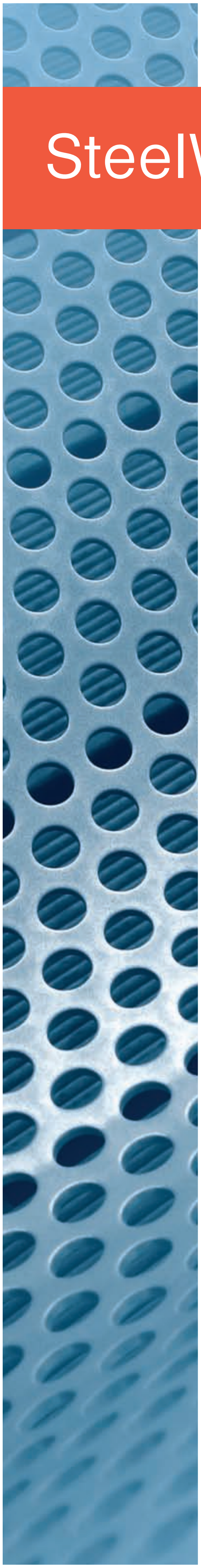
* When using Secure Browser, up to 600 users per GMM, 3600 users per GMC

** Activation Key acquired separately

*** Windows Server license included

MobileWorks is available through resellers worldwide and various contracting vehicles.

For more information call 800.296.3866
or visit us at www.steelcloud.com



SteelWorks® Fed*Mobile*™

BlackBerry® Enterprise Server 5 Solution for DoD

Delivering on the Promise of BES 5 with STIG Compliance and Easy Migration from BES 4.1 to 5

Fast and DoD-Ready

SteelWorks Fed*Mobile* is simply the best and quickest way to implement a STIG-compliant BlackBerry Enterprise Server appliance or cloud-based solution running under VMware. Why spend man-weeks migrating from version 4.1 to 5 while engineering your BlackBerry environment to be STIG-compliant when the SteelWorks FedMobile appliance can get you there in less than an hour? SteelCloud engineers have already implemented each of the hundreds of security guidelines mandated by Defense Information Security Agency's (DISA) STIGs to create a solution that is "Gold and Platinum Disk" compliant.

What is SteelWorks Fed*Mobile*?

SteelWorks Fed*Mobile* is an integrated hardware and software appliance or VMware-based virtual solution that comes pre-loaded with BlackBerry® Enterprise Server 5, hardened Windows Server OS, and SteelWorks' automated set-up and installation program. It enables any size DoD organization to easily upgrade from their current 4.1 environment or deploy a new STIG-compliant BlackBerry Enterprise Server at a fraction of the cost, time, and resource commitment normally required.

To maximize server availability and streamline ongoing maintenance tasks, SteelWorks Fed*Mobile* delivers advanced management features including Ever*Avail*™ for high availability and failover, disaster recovery and patch management. SteelCloud worked closely with Research In Motion (RIM) to create this unique "BES in a Box" appliance to eliminate the cost and time necessary to implement the 100's of pages of STIG requirements on your BlackBerry Enterprise Server 5.

Migrating from BES v4.1 to 5

SteelWorks *Transporter+*™ is a free tool that simplifies the migration of BlackBerry users from v4.1 to 5. The GUI interface lets you drag and drop users from their previous domain to their new one. In addition to the easy to use interface, *Transporter+* performs error checking to test and verify the move before it's committed.

Who else is using SteelWorks Fed*Mobile*?

Army, Navy and Air Force organizations have deployed SteelWorks Fed*Mobile*. In each case, administrators were able to start initializing BlackBerry Smartphones within hours of opening the box.

Benefits

- Reduces implementation time to 60 minutes vs. weeks or months.
- Eliminates the risk of non-compliance.
- Provides a standard configuration for all deployments.
- Simplifies ongoing maintenance tasks.
- Reduces time to migrate from v4.1 to 5.

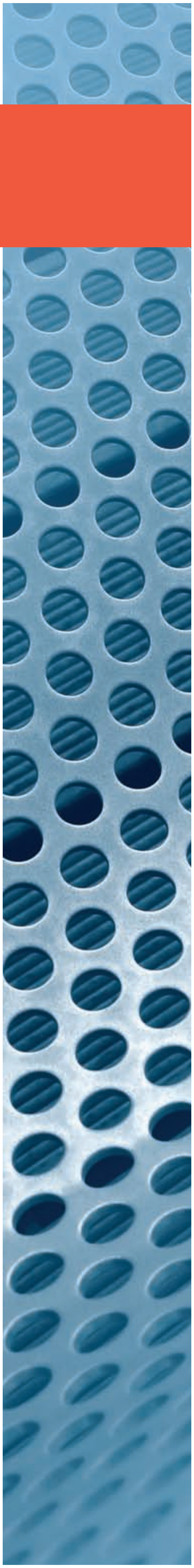
Features

- Delivered as a COTS solution.
- Available as an appliance or VMware-based virtual solution.
- Automated one-hour installation.
- Ever*Avail* provides a simple, 2 server self-healing high-availability configuration.
- STIGs are implemented for:
  - Wireless, including the BlackBerry Security Checklist
  - Windows Server OS
  - NET Framework
  - SQL
- Supports Microsoft® Exchange.
- SteelWorks Fed*Mobile* is "Gold and Platinum Disk" compliant.
- 3 year On-site warranty.
- Support for latest BlackBerry Smartphones.

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

vmware® READY

DISA



SteelWorks® Fed*Mobile*™

SteelWorks Fed*Mobile* VM at a Glance

SteelWorks FedMobile VM is a software-only solution that easily installs in an existing VM infrastructure to create a complete DISA STIG-compliant BlackBerry Enterprise Server environment. SteelCloud's virtual appliance also includes EverAvail™, a unique software suite for high availability, patch management, backup, and disaster recovery. SteelWorks FedMobile VM is designed to support both new installations of BlackBerry Enterprise Server 5, as well as migrations from previous versions.

All DoD organizations have a mandate to conform to certain Defense Information Security Agency (DISA) Security Technical Implementation Guides or "STIGs." SteelCloud's SteelWorks FedMobile VM is an enhanced implementation of its appliance for BlackBerry Enterprise Server that leverages the server's IT policies to provide a consistent pre-configured DoD STIG-compliant BlackBerry environment in under an hour, rather than weeks or months.

VMware provides a powerful, proven platform for delivering virtual infrastructures to DoD users. Based on our market leading FedMobile solution, SteelWorks FedMobile VM allows you to address today's critical IT issues such as server consolidation, test and development, and manageability and security in a BlackBerry Enterprise Server environment.

High Availability with Ever*Avail*™

From installation to operation to recovery, SteelWorks is much more than a BlackBerry Appliance. SteelWorks' innovative SteelWorks Ever*Avail*™ includes a set of advanced automated back-up and recovery utilities that simplify crucial daily back-up routines. With Ever*Avail* you quickly back-up the complete appliance image in the appliance itself (or on a network-shared drive), apply a patch, and then, if there is a problem, restore the system to a previous "snapshot" (even in the event of a Windows failure).

High Availability/Half the Cost – SteelWorks Ever*Avail*™ automated "self-healing" failover approach offers high-availability with only two appliances. Other approaches require four servers to do the job.

No matter how your internal IT support resources may change, you can be confident that SteelWorks Fed*Mobile* will deliver the performance, reliability and compliance your agency requires for secure Smartphone communications.

SteelWorks Fed*Mobile* Appliance Specifications

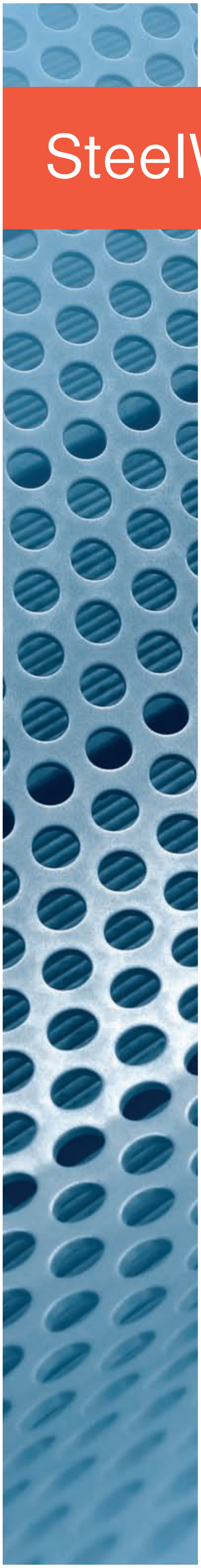
Model	Part	Appliances	# of Users	CPU	Memory	Form Factor	Included Software
E2400	SCLD-SW-STIG-E2443A	Single	Up to 500	Intel Xeon Quad Core	4 GB	1U 1.7" x 17.1" x 15.5"	BES 5*, Windows Server OS**, SteelWorks EverAvail™
	SCLD-DUAL-STIG-E2443A	Dual HA Pair					
E4400	SCLD-SW-STIG-E4446A	Single	Up to 1000	Intel Xeon Quad Core	4 GB	1U 1.7" x 17.6" x 16.7"	
	SCLD-DUAL-STIG-E4446A	Dual HA Pair					
E4800	SCLD-SW-STIG-E4886A	Single	Up to 2000	Intel Xeon 2x Quad Core	8 GB	1U 1.7" x 17.6" x 16.7"	
	SCLD-DUAL-STIG-E4886A	Dual HA Pair					

**Activation key acquired separately*

** *Windows Server license included*

Elite Alliance Member

SteelWorks FedMobile is available through resellers worldwide and various contracting vehicles. For more information call 800.296.3866 or visit us at www.steelcloud.com..



SteelWorks® STIG360™

Worry-free Lifecycle STIG Compliance for DoD BlackBerry® Enterprise Servers

Installing a STIG-compliant BlackBerry Enterprise Server (BES) can be time consuming, error prone and expensive. SteelCloud's FedMobile solutions make initial deployment of STIG-compliant BlackBerry Enterprise servers a snap for both server and virtualized infrastructures. But once BES is installed, the job is not over. It can take significant resources to keep your mobile environment compliant with the latest DISA STIGs for Windows Server, .NET, SQL, and BlackBerry Wireless. Our DoD customers have asked for help and SteelCloud has answered with STIG360 - our ongoing STIG compliance support program.

SteelCloud's new STIG360 offering provides ongoing security support services for SteelWorks FedMobile customers in order to remain STIG-compliant over the life of their BlackBerry Enterprise Server implementations. This program keeps our FedMobile customers up to date with all of the latest DISA STIGs necessary to stay in compliance. STIG360 includes STIG update notification, telephone support, online customer portal for access to SteelWorks STIG implementation guides, and software image upgrade/ replacement services.

STIG360 begins with pro-active notification when a new STIG is available. SteelCloud's specialized support portal is available, on a 24-hour basis, where you can access our STIG implementation guides, developed as step-by-step tutorials for updating your BES environment for the latest STIGs. These guides tell you the differences between the previous and current STIG(s) and will provide you with the steps, procedures and system commands required to get compliant with each new STIG. For questions, you can access our online support knowledgebase or simply call our support line where you will be connected to SteelCloud experts knowledgeable in Microsoft Exchange, Active Directory, BES, and each of the four STIGs required for a DISA compliant BES environment.

Take the worry out of STIG implementation. SteelWorks STIG360 was developed for DoD Information Assurance personnel and BlackBerry Enterprise Server administrators. We provide the information, tools, and services needed to remain compliant with the latest DISA mandated STIGs – with the least risk and at the lowest cost.

Features

- Pro-active notification of STIG updates
- STIG updates for:
  - Wireless Checklist
- Windows Server:
  - NET
  - SQL
- STIG Implementation Guides
- Automated installation when available
- FedMobile Appliance software support
- Software image updates/replacements
- 8x5 telephone support
- Online support portal

SteelWorks STIG360™ is available through resellers worldwide and various contracting vehicles. For more information call 800.296.3866 or visit us at www.steelcloud.com.

Complete Mobile

Risk Management

pre-configured for STIG compliance

Fixmo and SteelCloud® have formed a technology partnership to deliver Fixmo's industry-leading Sentinel™ mobile risk management solution in a pre-configured STIG-compliant (Security Technical Implementation Guidelines) SteelCloud SteelWorks® appliance.

Fixmo Sentinel

Mobile devices are an invaluable communications tool within government organizations. They also expose the organization to the threat of malicious attacks, tampering and other mobile risks. Fixmo Sentinel™ is a comprehensive end-to-end mobile risk management solution designed to mitigate risk throughout an enterprise device's lifecycle.

SteelCloud SteelWorks

All DoD organizations have a mandate to conform to certain Defense Information Security Agency (DISA) STIGs. The SteelWorks appliance saves organizations one to two months of highly technical security work configuring a STIG-compliant environment.

Fixmo Sentinel Features

Fixmo Sentinel provides a secure end-to-end mobile risk management solution designed to mitigate risk throughout a mobile device's lifecycle:

Device Assurance: Monitors device integrity and takes action if the device leaves a known trusted state.

Policy Compliance: Detects any changes to mobile device policies and configurations.

Device Audit: Documents the organization's compliance with regulatory policies.

SteelWorks Appliance Features

SteelWorks provides the quickest way to implement Fixmo Sentinel and is available as a server appliance or VMware solution:

Save Time & Money: Sentinel is pre-installed and pre-configured on an industry leading server appliance or VMware solution for plug and play DoD installation in as little as 60 minutes.

Eliminates the risk of non-compliance: Start Fixmo Sentinel on day one in a known STIG-compliant state.

Stay in compliance: With SteelCloud's unique STIG360 support program, it's easy to keep your Fixmo Sentinel system in STIG compliance - at the least possible cost and effort.

Fixmo

fixmo.com

Contact Fixmo to learn more about Fixmo Sentinel, a leading mobile risk management solution for enterprise mobile devices: sales@fixmo.com.

STEEL CLOUD®

steelcloud.com

Over 24 years, SteelCloud has won numerous awards for technical excellence and customer satisfaction: info@steelcloud.com